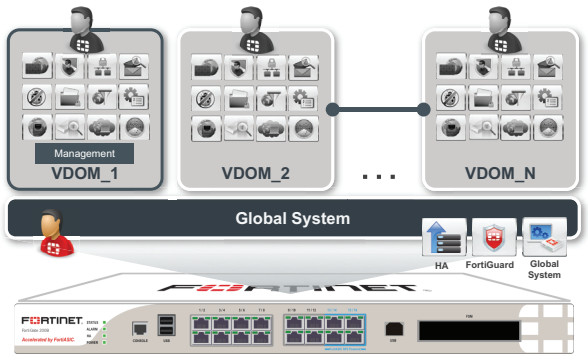
Virtual Domains (VDOMs)

Virtual domains are used to divide a single FortiGate unit into two or more virtual instances of FortiOS that function separately and can be managed independently.

What are VDOMs?



Virtual domains (VDOMs) divide a FortiGate security gateway into two or more (up to 250) virtual FortiGate devices, each operating as an independent FortiGate security gateway. Each VDOM can provide completely separate firewalling, routing, UTM, VPN, and next generation firewall services. All traffic enters and leaves a VDOM completely separated from traffic from other VDOMs.

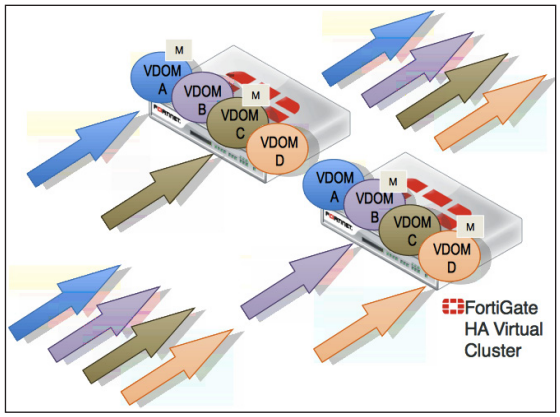
A multi-VDOM FortiGate unit can be centrally managed or individual VDOM administrators can manage their own VDOMs with no administrative access to other VDOMs. Management traffic, including DNS lookups, FortiManager access, FortiAnalyzer access, Syslog logging, sending alert emails, NTP, SNMP traps, and FortiGuard updates, are all handled from a separate management VDOM. If required, logging and reporting can be configured per-VDOM, allowing individual VDOM administrators to record and report on their VDOM's activities.

Transparent mode and NAT/Route mode VDOMS can be added to a single FortiGate device allowing both options on a network from a single platform. Traffic can also pass between VDOMs using inter-VDOM links. Inter-VDOM links allow administrators to apply different types of content inspection and other controls to the same traffic in different VDOMs. For example, traffic could be routed through a NAT/Route VDOM for routing following by a Transparent mode VDOM for UTM filtering. Inter-VDOM link traffic can also be accelerated by NP4 network processors available on many FortiGate models.

A reduced footprint

VDOMs are a green choice – they save space, energy, and money. With one FortiGate unit instead of ten or more, you have a reduced footprint in the server room, use less energy, and generate less heat. This reduced footprint is especially important for small companies renting co-located rack space in a shared data center.

The reduced footprint extends to lower management costs and reduced complexity. A multi-VDOM FortiGate device can be kept up-to-date with the latest firmware and UTM signatures just as easily as a single FortiGate unit. Firmware and UTM signature updates are centrally managed and are instantly available to all VDOMs.



Virtual Clustering

Virtual clustering is an extension of FortiGate high availability for a cluster of two FortiGate units with multiple VDOMs. Virtual clustering provides failover protection for a multiple VDOM configuration and can load balance traffic between the VDOMs to improve overall network performance.

Virtual clustering load balancing efficiently load balances all traffic between VDOMs (including TCP and UDP traffic, UTM traffic and VoIP traffic) and can be adjusted in real time to actively optimize load sharing between the cluster units without affecting the smooth operation of the VDOMs in the cluster.

System resource allocation

VDOMs must share the system resources of a single FortiGate unit. To ensure that no VDOM runs out of resources, configurable VDOM resource limiting optimizes the system resources available for each VDOM to ensure that each network or customer can rely on the service they expect. FortiGate administrators can allocate different resource levels in each VDOM according to required service levels.

Physical network interfaces

Firewalls normally need at least two interfaces to be useful. A large number of VDOMs would exceed the physical interface capacity of any FortiGate unit. To avoid running out of physical interfaces when configuring VDOMs, VLAN tagging can be used to segregate VDOM network traffic on shared physical interfaces.

VDOM licensing

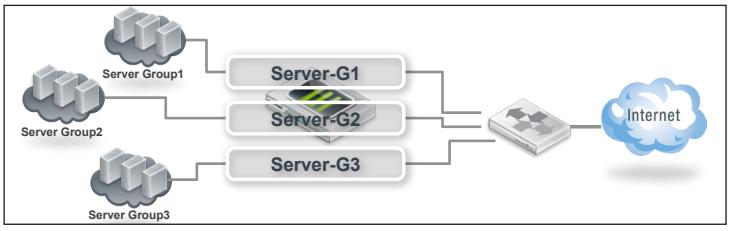
Most FortiGate units support up to 10 VDOMs. With an extended VDOM license, many FortiGate models can support up to 250 VDOMs. VDOM licenses are flexible and can be purchased for different numbers of VDOMs and extended to more VDOMs when required.

Example deployment scenarios

VDOMs can simplify a wide range of deployments that otherwise would require multiple security gateways.

Branch office deployment

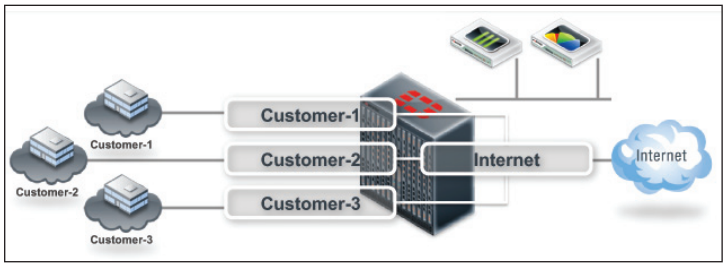
Organizations with branch offices may sometimes install multiple security gateways in their branch offices. One device acting as an Internet gateway, another for secure communication with HQ. These organizations can use VDOMS to consolidate security gateways into a single FortiGate device that includes a VDOM for Internet access and a VDOM for HQ access.



Data center deployment

Large and small data centers can use VDOMS in Transparent mode to add new UTM protection or other functionality to their data centers without disrupting current infrastructure. A FortiGate unit with multiple VDOMs in Transparent mode can provide different levels of UTM protection for different server groups or traffic steams, all from a single multi-VDOM FortiGate device. VDOMs can also be used in a data centre to provide security services for multiple servers, all from a single FortiGate unit.

MSP deployment



MPSs can use a single FortiGate unit to provide out of the box multi-tenant solutions for up to hundreds of customers. Each customer's network is connected to their own VDOM with their own configuration and their own separate traffic flow. The service provider can centrally manage the FortiGate unit, handling firmware and FortiGuard upgrades and other central management functions. Customers can manage their own VDOMs or as a value-added feature, individual VDOMs can be managed by the service provider.